Beaming

THE PRICE OF INSECURITY

The Cost of Business Cybercrime in 2023

www.beaming.co.uk

EXECUTIVE SUMMARY

- Beaming's research, indicates that over a quarter of UK businesses fell victim to some form of cyber attack in 2023. This equates to more than 1.5 million nationwide.
- While the number of businesses falling victim in 2023 was broadly similar to 2019 when we last ran an equivalent cybercrime study, the mix looks somewhat different. Victim rates declined for the largest and smallest businesses but soared among SMEs.
- Manufacturing and finance firms, which are the most sophisticated in using new technologies such as AI, automation and data analytics, were most frequently affected by cybercrime. Over 85% of companies surveyed in these sectors experienced breaches last year.
- Phishing, the use of deceptive emails, messages, or links to websites designed to trick people into performing actions that would expose a business to a breach, was the most common way businesses fell prey to cyber criminals in 2023.
- Cybercrime costs differ by attack type and business size and range from zero to more than £500,000 per incident. The typical cost, however, was just over £5,000. By extrapolating our findings across the UK business population, we have calculated that the total cost to businesses last year was £30.5 billion.
- This figure is 138% more than the £12.8 billion estimate we calculated using a similar methodology for 2019. Small businesses employing between 11 and 50 people experienced the most significant change – a fourfold cost increase.
- In addition to rising victim numbers and soaring costs, the emotional toll of cybercrime is increasing. Almost all leaders we surveyed at businesses who experienced cybercrime in 2023 said they suffered emotional distress following the attack.
- Finally, our study shows that businesses of all sizes have increased cybersecurity investments. Half of the leaders we surveyed said they now provide cybersecurity training for their employees, and the adoption of other sophisticated cybersecurity tools and approaches is accelerating.

INTRODUCTION

In an era of digital transformation and increasing reliance on technology, cybercrime poses a significant and escalating threat to businesses.

In January 2024, Beaming commissioned research consultancy Censuswide to interview UK business leaders about their approaches to cyber security and any breaches that affected their organisations in 2023.

Censuswide spoke to more than 500 leaders from organisations of all sizes, major sectors and UK regions, enabling us to understand how resilient they are to cybercrime today and what happens when cybercriminals succeed.

We also combined our findings with UK Government business population estimates to provide robust calculations showing the scale of cybercrime today and the cost to the UK economy.

We've shared our findings in this report to provide business leaders with new insight into the current state of cybercrime and help them counter the threat more effectively.

As the threat evolves and escalates, businesses must adapt their cybersecurity strategies to safeguard their assets, data and reputations.

Contents

THE RATE OF CYBERCRIME IN 2023

Cybercrime rates soar for UK SMES

Our research indicates that over a quarter (27%) of UK businesses, more than 1.5 million nationwide, fell victim to some form of cyber attack in 2023.

While the UK's four million solo businesses relying on just one person are not immune to cybercrime, the chances of becoming a victim triple when a company grows beyond a single individual. Our research shows that over half (57%) of businesses with between two and ten people suffered a cyber breach in 2023.

For businesses with over ten people, victim rates exceeded 80% in 2023.

The danger increases with size because businesses develop more extensive digital footprints as they grow. More staff, more devices, and more complex IT functions offer cybercriminals a comprehensive range of potential entry points to exploit and a wider attack surface.

Small businesses hold valuable data, including sensitive customer information, financial records, and intellectual property. The allure of such assets makes them prime targets for cybercriminals seeking financial gain or to leverage the acquired information for malicious purposes.

UK Business Cybercrime Rates and Costs

	All	Solo (1 person)	Micro (2 - 10)	Small (11 - 50)	Medium (51 -250)	Large (251+)
Proportion of businesses falling vitim in 2023	27%	15%	57%	83%	83%	82%
Estimated total number of businesses falling victim	1.52m	632k	665k	186k	31k	7k

Source: Beaming & Censuswide 2024

Number of SMEs falling victim to cybercrime up two-thirds since 2019

While the total proportion of UK businesses falling victim to cybercrime (27%) in 2023 was similar to when we last ran a cybercrime study at the end of 2019 (25%), the mix of businesses looks somewhat different.

The proportion of firms with over 250 people falling victim fell from 87% in 2019 to 82% last year, while victim rates for those with just one person declined from 21% to 15%.

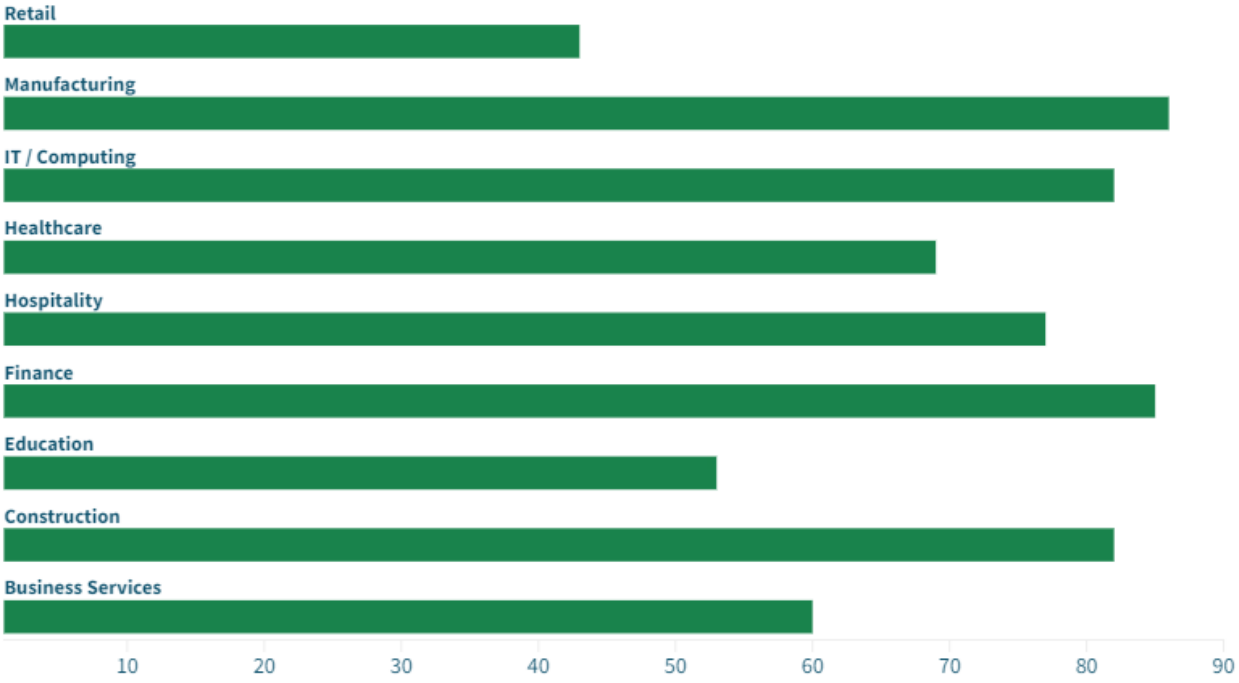
However, victim rates increased significantly for SMEs. In 2019, 39% of firms employing between two and 250 people (around 551,000 across the UK) fell victim to cybercrime. Last year, that had increased to 61% of SMEs, some 882,000 nationwide.

Manufacturing and finance firms have the highest cybercrime rates

Manufacturing and finance businesses were most frequently affected by cybercrime in 2023, with over 85% of companies surveyed in these sectors falling victim to a cyberattack last year.

Beaming's analysis shows that these sectors are also the most sophisticated in the use of new technologies such as AI, automation and data analytics[1]. Their IT environments were likely to have offered a more comprehensive range of potential entry points to exploit.

Proportion of Businesses Falling Victim by Sector in 2023



Source: Beaming & Censuswide 2024

[1] Beaming.co.uk, February 2024: Navigating the Tech Landscape - SME IT Adoption & Investment Plans for 2024

THE COST OF CYBERCRIME IN 2023

Cybercrime Cost UK Companies £30 Billion In 2023

We asked leaders of businesses that had fallen victim to cybercrime last year how much it cost them to manage each incident. Our study showed that the cost of incidents differed by the type of cybercrime and the size of the business affected, with the financial impact ranging from zero (6% of cases) to more than £500,000 (3% of cases).

We found that the average cost of cybercrime to victims in 2023 was just over £5,000.

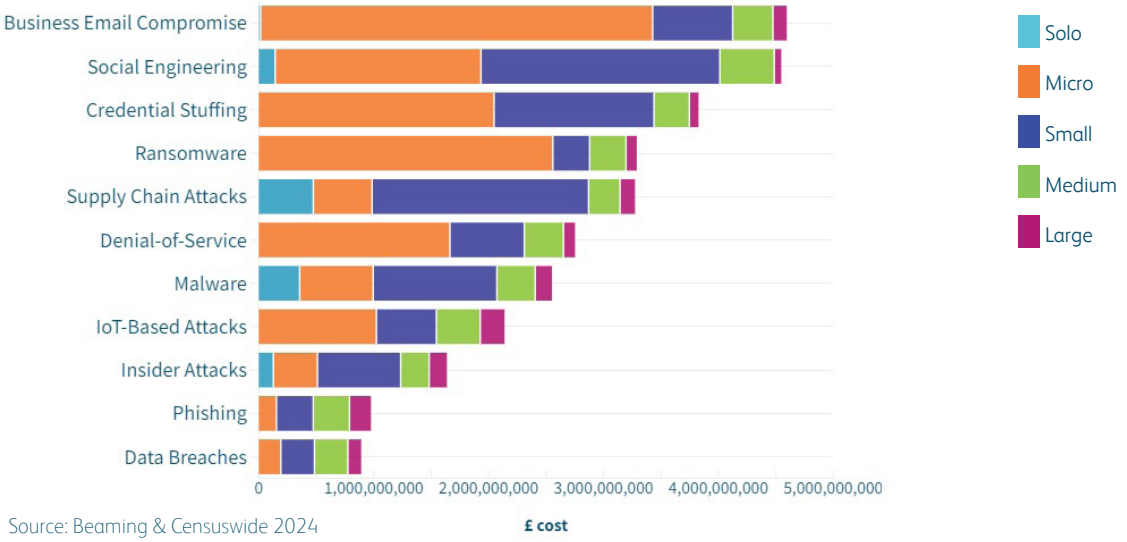
By extrapolating our findings using UK government business population estimates, we have calculated that the total cost of cybercrime to businesses last year was £30.5 billion[2].

This is a massive 138% increase on the £12.8 billion estimate we calculated using a similar methodology for 2019. The most significant increase was experienced by small businesses, for whom the cost of cybercrime has increased almost fourfold.

UK Business Cybercrime Rates and Cost

	All	Solo (1 person)	Micro (2 - 10)	Small (11 - 50)	Medium (51 -250)	Large (251+)
Typical cost of a cyber breach	£5.5k	<£1k	£12k	£45k	£98k	£176k
Estimated total cost across UK business population	£30.5bn	£1.1bn	£14.4bn	£10.0bn	£3.6bn	£1.4bn
Changes since 2019	138%	-74%	207%	396%	191%	118%

Total Cost of Cybercrime to UK Businesses in 2023



Source: Beaming & Censuswide 2024

[2] We asked leaders of breached businesses how much it cost them to manage each incident, including recovering data, replacing IT assets and people, and any financial penalties they incurred, as well as the impact of business interruption and any opportunities lost. To show the typical cost of incidents and calculate the total impact of cybercrime across the UK business community, we took median figures provided by business leaders for each cybercrime and size segment in our survey and multiplied them by the size of the relevant business populations. We took business population data from the UK Government's October 2023 estimates.

WHICH FORMS DID CYBERCRIME TAKE?

Phishing and malware claim more victims

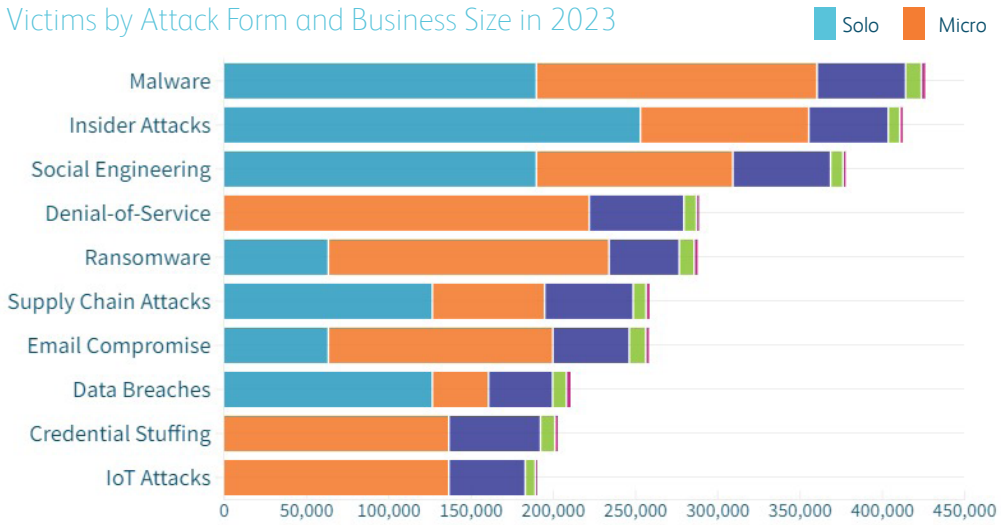
Our study reveals the forms of cyber attack businesses fell prey to most frequently in 2023:.

Phishing: The use of deceptive emails, messages, or links to websites designed to trick people into clicking on malicious links, download infected attachments, or share sensitive information was the most common way in which UK businesses fell prey to cyber criminals in 2023. We believe that around 679,000 UK businesses were compromised by phishing attacks last year, costing them almost £1 billion.

Malware: Malicious software designed to disrupt, damage or gain unauthorised access to IT systems was the second most common way businesses fell victim last year, claiming an estimated 426,000 victims across the UK and a bill worth almost £2.6 billion.

Insider Attacks: We estimate that 412,000 businesses lost sensitive information or suffered other cybersecurity issues due to employees or contractors in 2023. These attacks, which cost UK businesses an estimated £1.6 billion last year, can be malicious or accidental but still pose significant threats to security as insiders would already have a level of trust and access within the system.

Victims by Attack Form and Business Size in 2023



Find the cybercrime glossary on page 11

Source: Beaming & Censuswide 2024

Beaming's research identified several cyber attack methods that, although less common than those detailed above, have surged since we last surveyed leaders about cybercrime.

In 2019, 2% of businesses fell victim to social engineering, where criminals manipulate individuals into divulging confidential information or performing actions that compromise security. In 2023, that had risen to 7%, representing an increase from 122,000 victims a year to 378,000.

Over the same victim period, rates for ransomware and distributed denial of service attacks increased from just 1% of the business population to 5% each. Those represent increases of 63,000 to 288,000 ransomware victims and 77,000 to 289,000 denial of service victims over the last four years.

BEYOND THE COST OF A BREACH

The emotional toll of cybercrime is increasing

Most business leaders recognise that cybercrime can have a devastating impact on their finances and productivity. Our study shows that it can also have a harmful psychological effect.

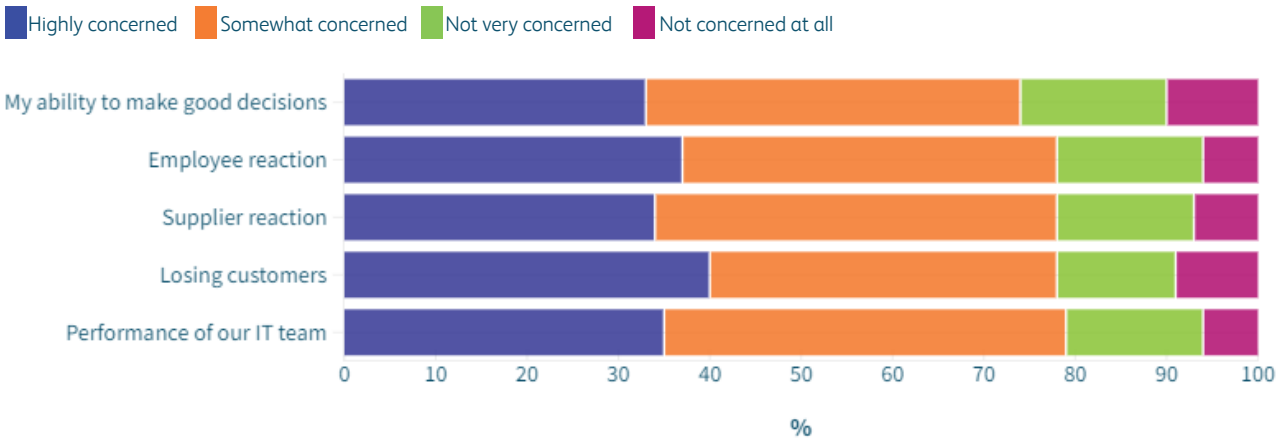
Almost all (90%) leaders we surveyed at businesses who experienced cybercrime in 2023 said they suffered some form of emotional distress following the attack, reporting symptoms more commonly associated with post-traumatic stress disorder (PTSD). This figure compares to 76% of leaders in 2019.

A third (32%) said they experienced anxiety as a result of the attack, and around a quarter admitted to feeling shocked (27%), angry (24%) or nervous (23%).

39% of leaders at firms that had suffered cybercrimes were 'highly concerned' about losing customers following their attack. 79% expressed at least a moderate level of concern about the performance of their IT departments.

The impact of cybercrime is such that it can be difficult to assess the full extent of a breach. Beyond the direct financial impact and the cost of lost opportunities, there are also indirect costs and impacts that can take much longer to fix than replacing IT assets or restoring data.

Additional concerns created by Cybercrime



Source: Beaming & Censuswide 2024

HOW CAN BUSINESSES PROTECT THEMSELVES?

Enhancing resilience to cyber threats

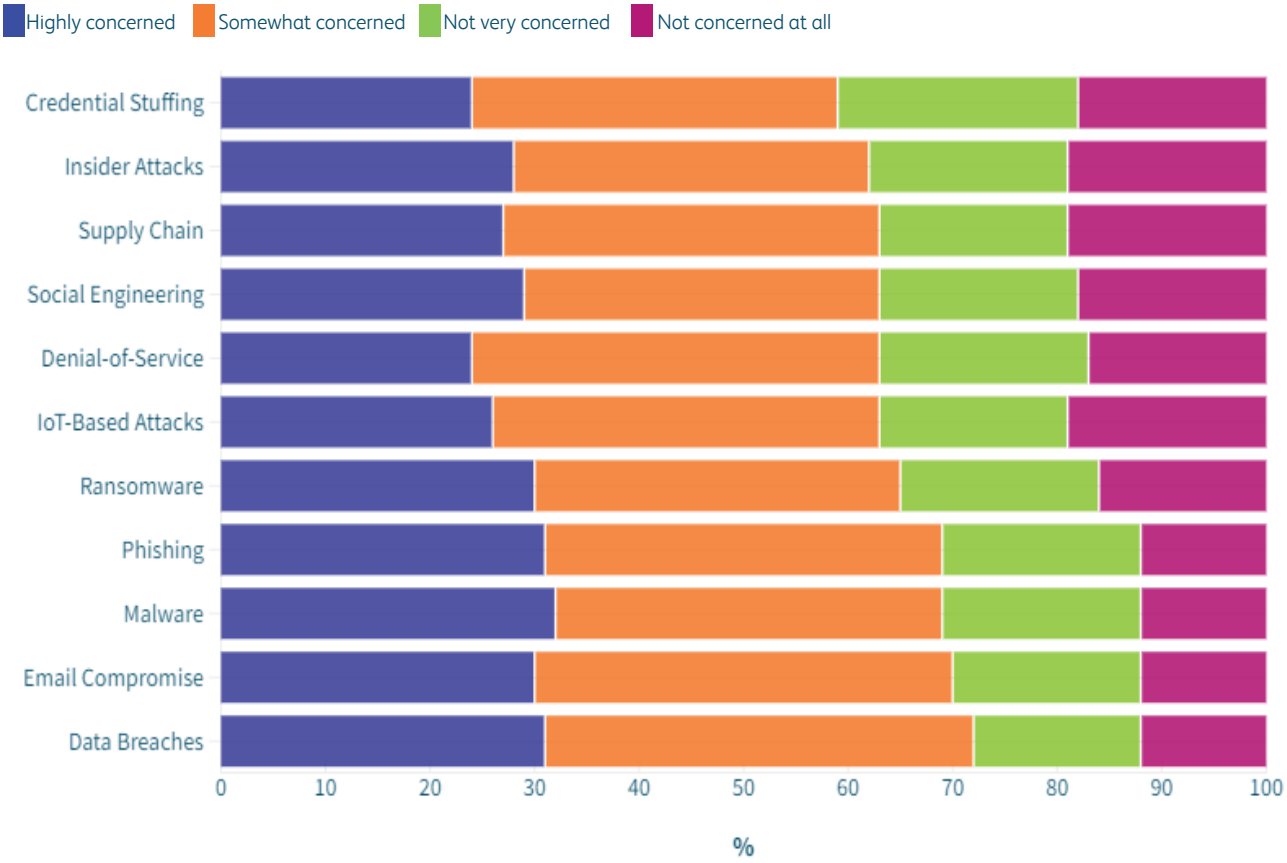
When it comes to cybercrime, it is clear that any form it takes is a concern for business leaders and that companies are taking more measures to guard against it.

Malware and phishing, the most likely ways for a company to fall victim, are among the top concerns, and quite rightly so. 32% of the leaders we surveyed said they were 'highly concerned' by malware, to the extent that they discussed it at board level and now take extensive measures to combat the threat.

The form of cybercrime raising most concerns, however, was data breaches. 72% of business leaders said they were 'somewhat' or 'highly' concerned about the threat of cybercriminals gaining unauthorised access to sensitive data such as customer information, intellectual property or employee records.

Data breaches top the list of leaders' cyber concerns despite being one of the least frequent and least costly forms of cybercrime. Leaders, it seems, are highly concerned about the UK's data protection laws, including the General Data Protection Regulation (GDPR), which can result in serious legal repercussions for breaches, and the potential for significant reputation damage.

Business concern by Cybercrime



Source: Beaming & Censuswide 2024

Our study shows increased levels of investment in cybersecurity tools and approaches:

Half (48%) of the leaders we surveyed said they provided **cybersecurity training** for their employees. This figure was up from just 11% in 2019 and looks likely to increase to 60% in 2024. It has never been more important to equip people with the knowledge, skills, and awareness necessary to protect business systems, networks and data given the high prevalence of phishing, insider attacks and social engineering.

More than half (53%) of businesses now use **Network Perimeter Firewalls**, which play a crucial role in securing a computer network by acting as a barrier between a trusted internal network and untrusted external networks, such as the Internet. Our study suggests the use of this technology will increase to 62% by the end of this year,

The adoption of **managed private networks** used to secure data transmitted between different locations has increased from 8% of businesses in 2019 to 53% today. These networks, usually set up and maintained by a specialist service provider, help secure remote access to company systems and protect sensitive information from interception and unauthorised access. Adoption is likely to increase to 63% of businesses in 2024.

Unified Threat Management devices, which simplify security management and improve protection by integrating multiple security functions into a single, unified platform, have seen a massive increase in adoption. These are used by 40% of businesses today. In 2019, that figure was just 1%.

40% of businesses now use site-to-site **VPN technology,** up from 5% in 2019. Typically the responsibility for this usually lies with the organisation's IT or network administrators.

CYBERCRIME GLOSSARY

Credential Stuffing: Cybercriminals use stolen or leaked login credentials from one service to gain unauthorised access to other accounts where individuals may have reused passwords.

Data Breaches: Unauthorised access to and theft of sensitive data, such as customer information, intellectual property, or employee records.

Distributed Denial-of-Service Attacks: Cybercriminals disrupt a business's online services by overwhelming them with traffic. This can lead to downtime, loss of revenue, and damage to a company's reputation.

Email Compromise: Cybercriminals gain access to a business email account and use it to impersonate executives or employees. They may then trick employees into transferring funds, revealing sensitive information, or performing other malicious actions.

Insider Attacks: Theft of sensitive information and other incidents resulting from employees or contractors with malicious intent, or accidental compromise of security.

IoT Attacks: Cybercriminals exploit vulnerabilities in connected 'Internet of Things' devices to gain unauthorised access to business networks or launch attacks.

Malware: Cybercriminals use malicious software, including viruses, worms, and trojans, to infect a business's systems, causing damage, stealing information, or allowing unauthorised access.

Phishing: Cybercriminals use deceptive emails, messages, or links to websites to trick individuals into providing sensitive information such as usernames, passwords, or financial details.

Ransomware: A type of malware that encrypts files on a victim's system, rendering them inaccessible. Cybercriminals then demand a ransom, usually in cryptocurrency, in exchange for the decryption key.

Social Engineering: Cybercriminals manipulate individuals into divulging confidential information or performing actions that compromise security. Can include pretexting, baiting, or quid pro quo tactics.

Supply Chain Attacks: Cybercriminals gain unauthorised access to systems or spread malware through a business's suppliers or partners